

## CLAIMS

1 1. A method for managing and displaying contact authentication in a peer-to-peer  
2 collaboration system wherein users may have multiple identities each with an  
3 associated display name, comprising:  
4 (a) on a graphic user interface, displaying a name conflict indicator next to a  
5 first and a second display name, which display names are associated with  
6 different identities and are equivalent;  
7 (b) in response to a selection of a display name with a name conflict indicator  
8 displayed next thereto, displaying all display names that are equivalent to  
9 the selected display name; and  
10 (c) providing a mechanism to resolve the name conflict between two  
11 conflicting display names.

1 2. The method of claim 1 wherein step (a) comprises computing a clean name from  
2 each display name and comparing clean names of two display names to  
3 determine if the two display names are equivalent.

1 3. The method of claim 1 wherein each contact identity has an authentication level  
2 associated therewith and wherein step (a) comprises:  
3 (a1) examining the authentication levels of all display names that are  
4 equivalent; and  
5 (a2) displaying name conflict indicators next to selected display names based  
6 on the examination in step (a1).

1 4. The method of claim 3 wherein step (a2) comprises displaying a name conflict  
2 indicator next to each display name associated with a contact identity whose  
3 authentication level (1) is less than the highest authentication/certification level of  
4 all contact identities with equivalent display names or (2) equals the highest

5 authentication/certification level to which at least two contact identities with  
6 equivalent display names have equal authentication levels.

1 5. The method of claim 3 further comprising:

2 (d) providing a security policy that determines the behavior of the  
3 collaboration system regarding communications with a contact based on  
4 the authentication level of that contact.

1 6. The method of claim 5 wherein step (d) comprises allowing a user of the  
2 collaboration system to determine the security policy.

1 7. The method of claim 5 wherein step (d) comprises allowing a system  
2 administrator to determine the security policy.

1 8. The method of claim 5 further comprising:

2 (e) warning a user based on the security policy when that user attempts to  
3 communicate with a contact having a predetermined authentication level.

1 9. The method of claim 5 further comprising:

2 (e) preventing a user from communicating with another user based on the  
3 security policy when the other user has a predetermined authentication  
4 level.

1 10. The method of claim 1 wherein step (b) comprises displaying a dialog box having  
2 all display names that are equivalent to the selected display name listed therein.

1 11. The method of claim 1 wherein step (c) comprises assigning an alias to one of  
2 the first and second display names which alias is not equivalent to either of the  
3 first and second display names and which alias replaces the one display name.

- 1 12. The method of claim 1 further comprising:  
2 (d) displaying an authentication indicator next to a display name that is not  
3 equivalent to another display name, which authentication indicator  
4 displays the authentication level of the associated contact.
- 1 13. The method of claim 12 wherein each contact can have one of a predetermined  
2 number of authentication levels and wherein the authentication indicator that is  
3 displayed is unique to one of the authentication levels.
- 1 14. A method for managing and displaying contact authentication in a peer-to-peer  
2 collaboration system wherein users may have multiple authentication and  
3 certification levels, including an unauthenticated and uncertified level,  
4 comprising:  
5 (a) setting a security policy that controls the behavior of the collaboration  
6 system based on the authentication and certification level;  
7 (b) in response to an attempt by a user to communicate with one or more  
8 contacts, compiling a list of unauthenticated and uncertified contacts with  
9 whom the user is attempting to communicate; and  
10 (c) warning the user and restricting the user from communicating with  
11 contacts with an unauthenticated and uncertified level based on the  
12 security policy.
- 1 15. The method of claim 14 wherein step (a) comprises a user setting the security  
2 policy that applies to that user.
- 1 16. The method of claim 14 wherein step (a) comprises a system administrator  
2 setting a security policy that applies to a user.

- 1 17. The method of claim 14 wherein step (c) comprises warning a user when the  
2 security policy is set to warn and the user attempts to communicate with an  
3 unauthenticated and uncertified contact.
- 1 18. The method of claim 14 wherein step (c) comprises preventing a user from  
2 communicating with an uncertified contact when the security policy is set to  
3 restrict and the user attempts to communicate with an uncertified contact.
- 1 19. The method of claim 14 wherein step (c) comprises allowing a user to  
2 communicate with an unauthenticated and uncertified contact when the security  
3 policy is set to allow without warning and the user attempts to communicate with  
4 an unauthenticated and uncertified contact.
- 1 20. The method of claim 14 wherein step (b) comprises:  
2 (b1) compiling a contact list of contacts with whom the user is attempting to  
3 communicate;  
4 (b2) checking the contact list to determine contacts that are not authenticated;  
5 (b3) checking the unauthenticated contacts to determine whether a certification  
6 policy applies to any unauthenticated contact; and  
7 (b4) placing an unauthenticated contact on the list of unauthenticated and  
8 uncertified contacts when no certification policy applies to that contact.
- 1 21. Apparatus for managing and displaying contact authentication in a peer-to-peer  
2 collaboration system wherein users may have multiple identities each with an  
3 associated display name, comprising:  
4 means for displaying on a graphic user interface, a name conflict indicator  
5 next to a first and a second display name, which display names are associated  
6 with different contact identities and are equivalent;

7 means responsive to a selection of a display name with a name conflict  
8 indicator displayed next thereto for displaying all display names that are  
9 equivalent to the selected display name; and  
10 a mechanism that resolves the name conflict between two conflicting  
11 display names.

1 22. The apparatus of claim 21 wherein the means for displaying a name conflict  
2 indicator comprises a mechanism that computes a clean name from each display  
3 name and a comparator that compares the clean names of two display names to  
4 determine if the two display names are equivalent.

1 23. The apparatus of claim 21 wherein each contact identity has an authentication  
2 level associated therewith and wherein the means for displaying a name conflict  
3 indicator comprises:

4 means for examining the authentication levels of all display names that  
5 are equivalent; and

6 means for displaying name conflict indicators next to selected display  
7 names based on display names that are determined to be equivalent by the  
8 means for examining the authentication levels.

1 24. The apparatus of claim 23 wherein the means for displaying name conflict  
2 indicators next to selected display names comprises means for displaying a  
3 name conflict indicator next to each display name associated with a contact  
4 identity whose authentication level (1) is less than the highest  
5 authentication/certification level of all contact identities with equivalent display  
6 names or (2) equals the highest authentication/certification level to which at least  
7 two contact identities with equivalent display names have equal authentication  
8 levels.

1 25. The apparatus of claim 23 further comprising:

2 a mechanism that provides a security policy that determines the behavior  
3 of the collaboration system regarding communications with a contact based on  
4 the authentication level of that contact.

1 26. The apparatus of claim 25 wherein a mechanism that provides the security policy  
2 comprises a mechanism that allows a user of the collaboration system to  
3 determine the security policy.

1 27. The apparatus of claim 25 wherein the mechanism that provides the security  
2 policy comprises a mechanism that allows a system administrator to determine  
3 the security policy.

1 28. The apparatus of claim 25 further comprising:  
2 a mechanism that warns a user based on the security policy when that  
3 user attempts to communicate with a contact having a predetermined  
4 authentication level.

1 29. The apparatus of claim 25 further comprising:  
2 a mechanism that prevents a user from communicating with another user  
3 based on the security policy when the other user has a predetermined  
4 authentication level.

1 30. The apparatus of claim 21 wherein the means for displaying all display names  
2 that are equivalent to the selected display name comprises means for displaying  
3 a dialog box having all display names that are equivalent to the selected display  
4 name listed therein.

1 31. The apparatus of claim 21 wherein the a mechanism that resolves the name  
2 conflict comprises a mechanism for assigning an alias to one of the first and

3 second display names which alias is not equivalent to either of the first and  
4 second display names and which alias replaces the one display name.

1 32. The apparatus of claim 21 further comprising:

2 a mechanism that displays an authentication indicator next to a display  
3 name that is not equivalent to another display name, which authentication  
4 indicator displays the authentication level of the associated contact.

1 33. The apparatus of claim 32 wherein each contact can have one of a  
2 predetermined number of authentication levels and wherein the authentication  
3 indicator that is displayed is unique to one of the authentication levels.

1 34. Apparatus for managing and displaying contact authentication in a peer-to-peer  
2 collaboration system wherein users may have multiple authentication and  
3 certification levels, including an unauthenticated and uncertified level,  
4 comprising:

5 a mechanism that sets a security policy that controls the behavior of the  
6 collaboration system based on the authentication and certification level;

7 means responsive to an attempt by a user to communicate with one or  
8 more contacts for compiling a list of unauthenticated and uncertified contacts with  
9 whom the user is attempting to communicate; and

10 a mechanism that warns the user and restricts the user from  
11 communicating with contacts with an unauthenticated and uncertified level based  
12 on the security policy.

1 35. The apparatus of claim 34 wherein the mechanism that sets the security policy  
2 comprises a mechanism that allows a user to set the security policy that applies  
3 to that user.

1 36. The apparatus of claim 34 wherein the mechanism that sets the security policy  
2 comprises a mechanism that allows a system administrator to set a security  
3 policy that applies to a user.

1 37. The apparatus of claim 34 wherein the mechanism that warns the user and  
2 restricts the user comprises a mechanism that warns a user when the security  
3 policy is set to warn and the user attempts to communicate with an  
4 unauthenticated and uncertified contact.

1 38. The apparatus of claim 34 wherein the mechanism that warns the user and  
2 restricts the user comprises a mechanism that prevents a user from  
3 communicating with an uncertified contact when the security policy is set to  
4 restrict and the user attempts to communicate with an uncertified contact.

1 39. The apparatus of claim 34 wherein the mechanism that warns the user and  
2 restricts the user comprises a mechanism that allows a user to communicate with  
3 an unauthenticated and uncertified contact when the security policy is set to  
4 allow without warning and the user attempts to communicate with an  
5 unauthenticated and uncertified contact.

1 40. The apparatus of claim 34 wherein the means for compiling a list of  
2 unauthenticated and uncertified contacts comprises:  
3 means for compiling a contact list of contacts with whom the user is  
4 attempting to communicate;  
5 means for checking the contact list to determine contacts that are not  
6 authenticated;  
7 means for checking the unauthenticated contacts to determine whether a  
8 certification policy applies to any unauthenticated contact; and



9 means for placing an unauthenticated contact on the list of  
10 unauthenticated and uncertified contacts when no certification policy applies to  
11 that contact.

1 41. A computer program product for managing and displaying contact authentication  
2 in a peer-to-peer collaboration system wherein users may have multiple identities  
3 each with an associated display name, the computer program product comprising  
4 a computer usable medium having computer readable program code thereon,  
5 including:

6 program code for displaying on a graphic user interface a name conflict  
7 indicator next to a first and a second display name, which display names are  
8 associated with different contact identities and are equivalent;

9 program code operable in response to a selection of a display name with a  
10 name conflict indicator displayed next thereto, for displaying all display names  
11 that are equivalent to the selected display name; and

12 program code that provides a mechanism to resolve the name conflict  
13 between two conflicting display names.

1 42. A computer program product for managing and displaying contact authentication  
2 in a peer-to-peer collaboration system wherein users may have multiple  
3 authentication and certification levels, including an unauthenticated and  
4 uncertified level, the computer program product comprising a computer usable  
5 medium having computer readable program code thereon, including:

6 program code for setting a security policy that controls the behavior of the  
7 collaboration system based on the authentication and certification level;

8 program code operable in response to an attempt by a user to  
9 communicate with one or more contacts, for compiling a list of unauthenticated  
10 and uncertified contacts with whom the user is attempting to communicate; and

11           program code for warning the user and restricting the user from  
12           communicating with contacts with an unauthenticated and uncertified level based  
13           on the security policy.